GIDS

De complete gids voor IoT & OT Security

IT/OT convergentie, IEC 62443, NIS2, dreigingen en kosten. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De dreiging voor IoT- en OT-omgevingen groeit explosief. Deze cijfers laten zien waarom actie urgent is.

820.000
IoT-aanvallen per dag gemiddeld in 2025
DeepStrike [1]

332%
toename internet-blootgestelde OT-apparaten
Palo Alto Networks 2026 [2]

64%
stijging in ransomwaregroepen die industriele organisaties targeten
Nozomi Networks 2025 [3]

75%
van connected medical devices draait op een verouderd besturingssysteem
Forescout 2025 [4]

44%
van alle datalekken bevat ransomware (2025)
Verizon DBIR 2025 [5]

66%
van manufacturing breaches bevat malware -- was 40--50%
Verizon DBIR 2025 [5]

20M
OT-gerelateerde services zichtbaar op het publieke internet
Palo Alto Networks 2026 [2]

Q2 2026
verwachte inwerkingtreding Cyberbeveiligingswet -- OT-sectoren in scope
NCSC [6]

1. Wat is IoT & OT Security?

IoT & OT Security omvat de beveiliging van Internet of Things-apparaten en Operational Technology-systemen tegen cyberaanvallen.

Operational Technology (OT) zijn de systemen die fysieke processen aansturen: SCADA-systemen, PLC's, sensoren en actuatoren in fabrieken, energiecentrales, waterzuivering en transportnetwerken. IoT-apparaten -- van beveiligingscamera's tot slimme sensoren -- voegen duizenden nieuwe endpoints toe aan het netwerk.

Het probleem: OT-systemen zijn ontworpen voor beschikbaarheid en betrouwbaarheid, niet voor security. Ze draaien vaak decennialang op verouderde software, gebruiken protocollen zonder authenticatie (Modbus, DNP3), en zijn steeds vaker verbonden met IT-netwerken en het internet [3].

2. Waarom is het belangrijk?

De convergentie van IT en OT creert een aanvalsoppervlak dat ransomwaregroepen actief exploiteren.

Het aantal ransomwaregroepen dat industriele organisaties target steeg met 64% -- van 80 naar 119 groepen [3]. De exploitatie van edge devices en VPNs (de brug tussen IT en OT) steeg van 3% naar 22% van vulnerability-breaches [5]. En er zijn nu 20 miljoen OT-gerelateerde services zichtbaar op het publieke internet [2].

De financiele impact is enorm: downtime in productieomgevingen kost EUR 5.000--50.000 per uur. Een ransomware-aanval op een industriele omgeving kan wekenlange uitval betekenen. In de gezondheidszorg kost een datalek gemiddeld USD 10 miljoen [7].

> **Business case:** Een basis IoT/OT scan kost EUR 2.500--8.000. Een uur productie-uitval kost EUR 5.000--50.000. De investering is terugverdiend als je een enkel incident voorkomt.

3. Hoe werkt het? Het beveiligingsproces

OT-beveiliging volgt een andere aanpak dan IT-security. Beschikbaarheid gaat voor vertrouwelijkheid.

1 Asset discovery en inventarisatie

WEEK 1--3

Breng alle IoT- en OT-apparaten in kaart: type, firmware, netwerklocatie, eigenaar. Gebruik passieve discovery om productiesystemen niet te verstoren.

2 Netwerksegmentatie

WEEK 2--5

Scheid IT- en OT-netwerken. Implementeer een DMZ (demilitarized zone) als tussenlaag. Microsegmentatie binnen OT voor kritieke systemen.

3 Risicobeoordeling en kwetsbaarheidsscan

WEEK 3--6

Voer een risicobeoordeling uit op basis van IEC 62443 Security Levels. Scan passief op bekende kwetsbaarheden (CVE's). Prioriteer op basis van impact.

4 Monitoring implementeren

WEEK 5--8

Implementeer passieve OT-monitoring: detectie van anomalieen in OT-verkeer, ongeautoriseerde wijzigingen en verdacht gedrag. Integreer met IT-security monitoring (SIEM).

5 Incident response en onderhoud

DOORLOPEND

Stel een OT-specifiek incident response plan op. Train OT-operators. Patch waar mogelijk, compenseer met segmentatie waar niet. Evalueer periodiek.

4. Wat kost het?

TIER	OMSCHRIJVING	PRIJSINDICATIE	EENHEID
Basis	IoT/OT security scan: asset inventaris, netwerksegmentatie review, quickscan kwetsbaarheden	EUR 2.500 -- 8.000	per assessment
Standaard	Volledige OT assessment: IEC 62443 gap-analyse, risicobeoordeling, segmentatie-ontwerp, roadmap	EUR 10.000 -- 35.000	per assessment
Premium	Managed IoT/OT security: continue monitoring, anomaly detection, incident response, compliance	EUR 3.000 -- 12.000	per maand

MKB-TIP

Begin met een IoT/OT security scan (EUR 2.500--8.000). De meeste organisaties ontdekken hiermee onbekende apparaten, open poorten en ontbrekende segmentatie. Dit geeft direct inzicht in de urgentie van vervolgstappen.

5. Waar moet je op letten bij een aanbieder?

- **OT-specifieke ervaring** -- IT-security is geen OT-security. Vraag naar ervaring met SCADA, PLC's en industriele protocollen
- **Passieve monitoring** -- Actieve scans kunnen OT-systemen verstoren. De aanbieder moet passief kunnen werken
- **IEC 62443 kennis** -- De standaard voor industriele cybersecurity
- **Beschikbaarheid als prioriteit** -- In OT gaat uptime voor; de aanbieder moet dit begrijpen
- **Sector-ervaring** -- Elke industriele sector heeft eigen risico's en regelgeving

> **RED FLAGS**
>
> Wees alert als een aanbieder: actieve vulnerability scans wil uitvoeren op productie-OT, alleen IT-security ervaring heeft, IEC 62443 niet kent, of geen rekening houdt met beschikbaarheidseisen.

6. Veelgemaakte fouten

1. IT-security maatregelen 1-op-1 kopieren naar OT

Antivirus op een PLC installeren of automatische updates forceren op SCADA-systemen kan productieprocessen verstoren. OT vereist een andere aanpak: segmentatie, monitoring en compenserende maatregelen.

2. Legacy systemen negeren

OT-systemen draaien vaak 15--30 jaar. "We vervangen het toch binnenkort" is geen beveiligingsstrategie. Segmenteer en monitor legacy systemen tot vervanging daadwerkelijk plaatsvindt.

3. Geen asset inventaris bijhouden

De meeste organisaties weten niet precies welke OT- en IoT-apparaten in hun netwerk zitten. Zonder inventaris kun je niet beveiligen.

4. OT-security als IT-verantwoordelijkheid zien

OT-beveiliging vereist samenwerking tussen IT, operations en management. Het is geen IT-project, maar een organisatiebrede verantwoordelijkheid.

5. Geen OT-specifiek incident response plan

Een IT-incident response plan werkt niet voor OT. Isoleren van een gecompromitteerde PLC heeft andere consequenties dan het uitschakelen van een server.

7. Compliance: NIS2, IEC 62443 en regelgeving

NIS2 / CYBERBEVEILIGINGSWET

Sectoren met OT-systemen -- energie, transport, industrie, water, zorg -- zijn expliciet benoemd als essential of important entities [6]. IoT-apparaten vallen technisch onder de scope, maar worden vaak niet meegenomen in risicobeoordelingen. Boetes tot EUR 10 miljoen of 2% van jaaromzet.

IEC 62443

De internationale standaard voor het beveiligen van Industrial Automation and Control Systems (IACS). Definieert Security Levels (SL 1--4) en biedt een praktisch pad naar NIS2-compliance voor OT-omgevingen [8].

EU CYBER RESILIENCE ACT (CRA)

Maakt fabrikanten van connected products (inclusief IoT-apparaten) verantwoordelijk voor security gedurende de hele levenscyclus. Verwachte inwerkingtreding: 2027.

8. Verschil met verwante oplossingen

DISCIPLINE	FOCUS	VERSCHIL MET IOT/OT SECURITY
IoT/OT Security	Beveiliging van industriele en IoT-systemen	Specifiek gericht op OT-protocollen, beschikbaarheid en fysieke processen
Network Security	Beveiliging van IT-netwerken	IoT/OT Security gaat verder: OT-protocollen, passieve monitoring, safety
Endpoint Security	Beveiliging van endpoints (laptops, servers)	OT-endpoints (PLC's, sensoren) vereisen een andere aanpak
Vulnerability Management	Beheer van kwetsbaarheden	In OT is patching vaak niet mogelijk; compenserende maatregelen zijn nodig

9. Trends 2025--2026

IT/OT Convergentie

De integratie van IT- en OT-netwerken versnelt door Industry 4.0 en digitalisering. Dit vergroot het aanvalsoppervlak en vereist unified security monitoring die zowel IT- als OT-verkeer begrijpt.

OT-specifieke Ransomware

Ransomwaregroepen ontwikkelen steeds vaker malware die specifiek OT-protocollen en PLC's target. Malware in manufacturing breaches steeg naar 66% [5].

Edge Device Exploitatie

VPNs en edge devices -- vaak de brug tussen IT en OT -- zijn het primaire doelwit geworden. Exploitatie steeg van 3% naar 22% als aanvalsvector [5].

10. Aan de slag

DRIE DIRECTE ACTIES

1. Maak een inventaris van alle IoT- en OT-apparaten in je netwerk
2. Controleer of je IT- en OT-netwerken gesegmenteerd zijn
3. Plan een IoT/OT security scan om je specifieke risico's te identificeren

Hulp nodig? Op ibgids.nl/word-gematcht word je vrijblijvend gematcht met IoT/OT security specialisten die passen bij jouw sector en omgeving.

Bronnenlijst

[1] **DeepStrike IoT Hacking Statistics 2025** -- deepstrike.io/blog/iot-hacking-statistics

[2] **Palo Alto Networks OT Security Report 2026** -- live.paloaltonetworks.com/t5/community-blogs/strengthen-operational-resilience-against-targeted-ot-threats/ba-p/1248890

[3] **Nozomi Networks OT/IoT Trends 2025** -- nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2025

[4] **Forescout 2025 Device Vulnerability Report** -- industrialcyber.co/reports/forescouts-2025-report-reveals-surge-in-device-vulnerabilities-across-it-iot-ot-and-iomt/

[5] **Verizon DBIR 2025** -- verizon.com/business/resources/reports/dbir/

[6] **NCSC Cyberbeveiligingswet (NIS2)** -- ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[7] **IBM Cost of Data Breach Report 2025** -- ibm.com/reports/data-breach

[8] **DNV IEC 62443 NIS2 Compliance** -- dnv.com/cyber/insights/articles/leverage-iec-62443-for-eu-nis2-directive-compliance/

[9] **NCSC OT/IACS Beveiliging** -- ncsc.nl/wat-kun-je-zelf-doen/technologische-ontwikkelingen/iacs-ot/aan-de-slag-met-het-beveiligen-van-ot-iacs

[10] **CBS Cybersecuritymonitor 2024** -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[11] **ENISA Threat Landscape 2025** -- enisa.europa.eu/publications/enisa-threat-landscape-2025

[12] **PwC Digital Trust Insights 2026** -- industrialcyber.co/reports/pwcs-2026-global-digital-trust-insights-report-flags-ot-iiot-and-talent-gaps-as-top-cybersecurity-challenges/

[13] **ShieldWorkz IEC 62443 NIS2** -- shieldworkz.com/blogs/achieving-nis2-compliance-via-the-iec-62443-framework

[14] **ICT Group Defender for IoT Scan** -- ict.eu/en/products/be-sure-start-defender-iot-scan

[15] **Secura Industrial IoT Testing** -- secura.com/nl/services/iot/industrieel